CS 489 / 698: Software and Systems Security

Module 5: Non-technical Aspects of Security

ethics and legal issues

Meng Xu *(University of Waterloo)*

Winter 2024

Outline

Motivation

- The course content includes a wide range of attacks.
- These attacks can have societal impacts and individual impacts.
- Your future work, being it research, industry, start-ups, software, security, ..., depends on your awareness of legal and ethical issues.

Cambridge Analytica

Facebook–Cambridge Analytica data scandal

A timeline of the Cambridge Analytica scandal

A timeline of the Cambridge Analytica scandal

- In 2010, Facebook launched Open Graph. External developers can reach out to FB users and request access to not only their personal data, but also their friends' personal data too!

A timeline of the Cambridge Analytica scandal

- In 2010, Facebook launched Open Graph. External developers can reach out to FB users and request access to not only their personal data, but also their friends' personal data too!
- In 2013, an app "thisisyourdigitallife" approached to almost 300,000 users and paid them to take a psychological test.

A timeline of the Cambridge Analytica scandal

- In 2010, Facebook launched Open Graph. External developers can reach out to FB users and request access to not only their personal data, but also their friends' personal data too!
- In 2013, an app "thisisyourdigitallife" approached to almost 300,000 users and paid them to take a psychological test.
- In 2014, Facebook adapted its rules to limit a developer's access to user data, especially the friends' data.

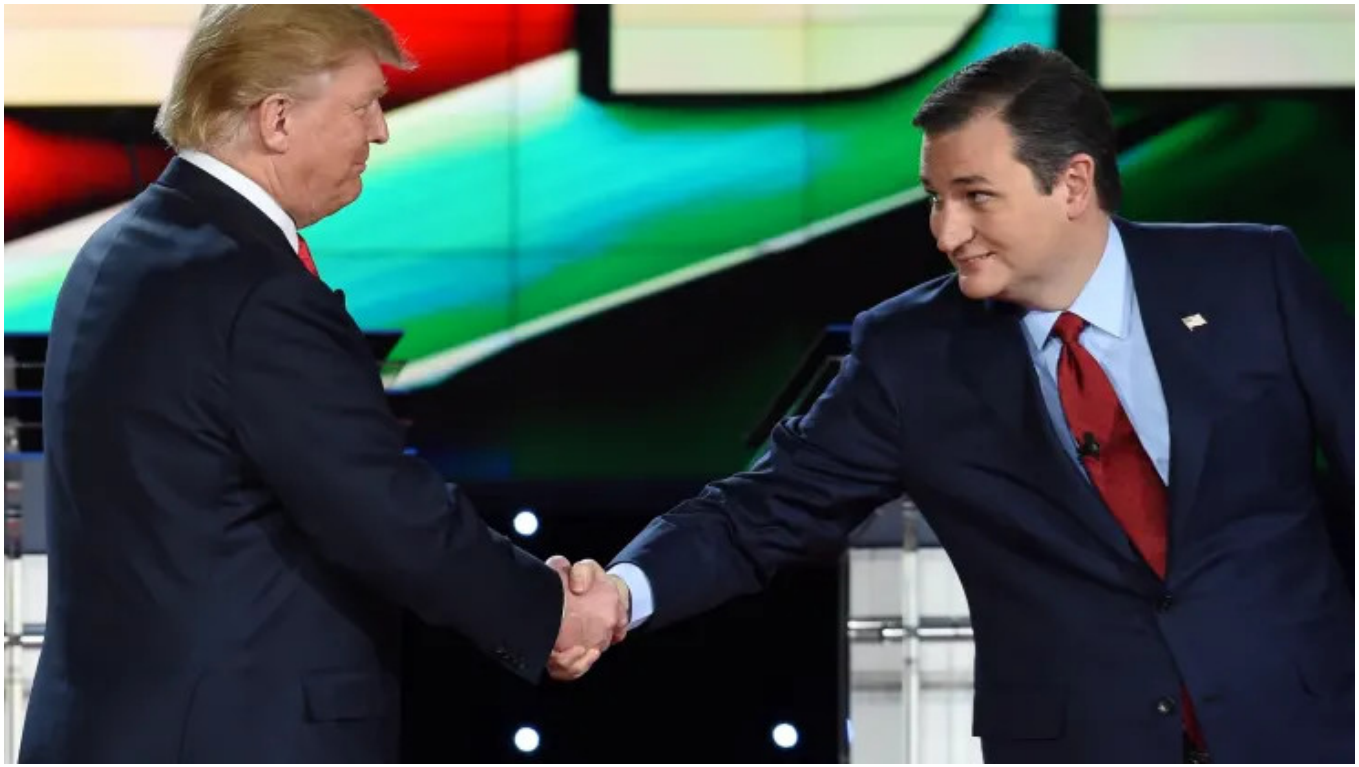
A timeline of the Cambridge Analytica scandal

- In 2010, Facebook launched Open Graph. External developers can reach out to FB users and request access to not only their personal data, but also their friends' personal data too!
- In 2013, an app "thisisyourdigitallife" approached to almost 300,000 users and paid them to take a psychological test.
- In 2014, Facebook adapted its rules to limit a developer's access to user data, especially the friends' data.
- In 2015, The Guardian reported that Cambridge Analytica was helping Ted Cruz's presidential campaign. FB acknowledged the data leak and argued that they have legally pressured Cambridge Analytica to remove all of the data they had improperly acquired.

A timeline of the Cambridge Analytica scandal

- In 2010, Facebook launched Open Graph. External developers can reach out to FB users and request access to not only their personal data, but also their friends' personal data too!
- In 2013, an app "thisisyourdigitallife" approached to almost 300,000 users and paid them to take a psychological test.
- In 2014, Facebook adapted its rules to limit a developer's access to user data, especially the friends' data.
- In 2015, The Guardian reported that Cambridge Analytica was helping Ted Cruz's presidential campaign. FB acknowledged the data leak and argued that they have legally pressured Cambridge Analytica to remove all of the data they had improperly acquired.
- In 2016, Cambridge Analytica was responsible for the "Defeat Crooked Hilary" video campaign on FB (assisting Trump's team).

A timeline of the Cambridge Analytica scandal



Donald Trump and Ted Cruz shake hands before the start of the Republican Presidential Debate (2015)

A timeline of the Cambridge Analytica scandal

Christopher Wylie, whistleblower of the Cambridge Analytica scandal

A timeline of the Cambridge Analytica scandal

- In March 2018, the scandal is exposed by The Guardian and The New York Times. The initial number is 50 million user profiles and later revised to 87 million (estimated by FB).

A timeline of the Cambridge Analytica scandal

- In March 2018, the scandal is exposed by The Guardian and The New York Times. The initial number is 50 million user profiles and later revised to 87 million (estimated by FB).
- In March 2018, Mark Zuckerberg first apologized for the situation, calling it an “issue”, a “mistake” and a “breach of trust”

A timeline of the Cambridge Analytica scandal

- In March 2018, the scandal is exposed by The Guardian and The New York Times. The initial number is 50 million user profiles and later revised to 87 million (estimated by FB).
- In March 2018, Mark Zuckerberg first apologized for the situation, calling it an "issue", a "mistake" and a "breach of trust"
- In July 2018, United Kingdom's Information Commissioner's Office announced to fine FB £500,000 ($663,000)
- In July 2019, the Federal Trade Commission announced to fine FB around $5 billion to settle the data breach investigation
- In July 2019, the Securities and Exchange Commission announced to fine FB around $100 million for misleading investors about potential risks it faced from misuse of user data

Linux kernel and the University of Minnesota

Linux kernel and the University of Minnesota

- You are an open-source enthusiast and make contributions to open-source projects regularly

Linux kernel and the University of Minnesota

- You are an open-source enthusiast and make contributions to open-source projects regularly
- You are deeply concerned that the Linux kernel might be vulnerable to supply chain attacks due to its loose review process

Linux kernel and the University of Minnesota

- You are an open-source enthusiast and make contributions to open-source projects regularly
- You are deeply concerned that the Linux kernel might be vulnerable to supply chain attacks due to its loose review process
- You want to remind the code reviewers that they should tight-up their code review practices

Linux kernel and the University of Minnesota

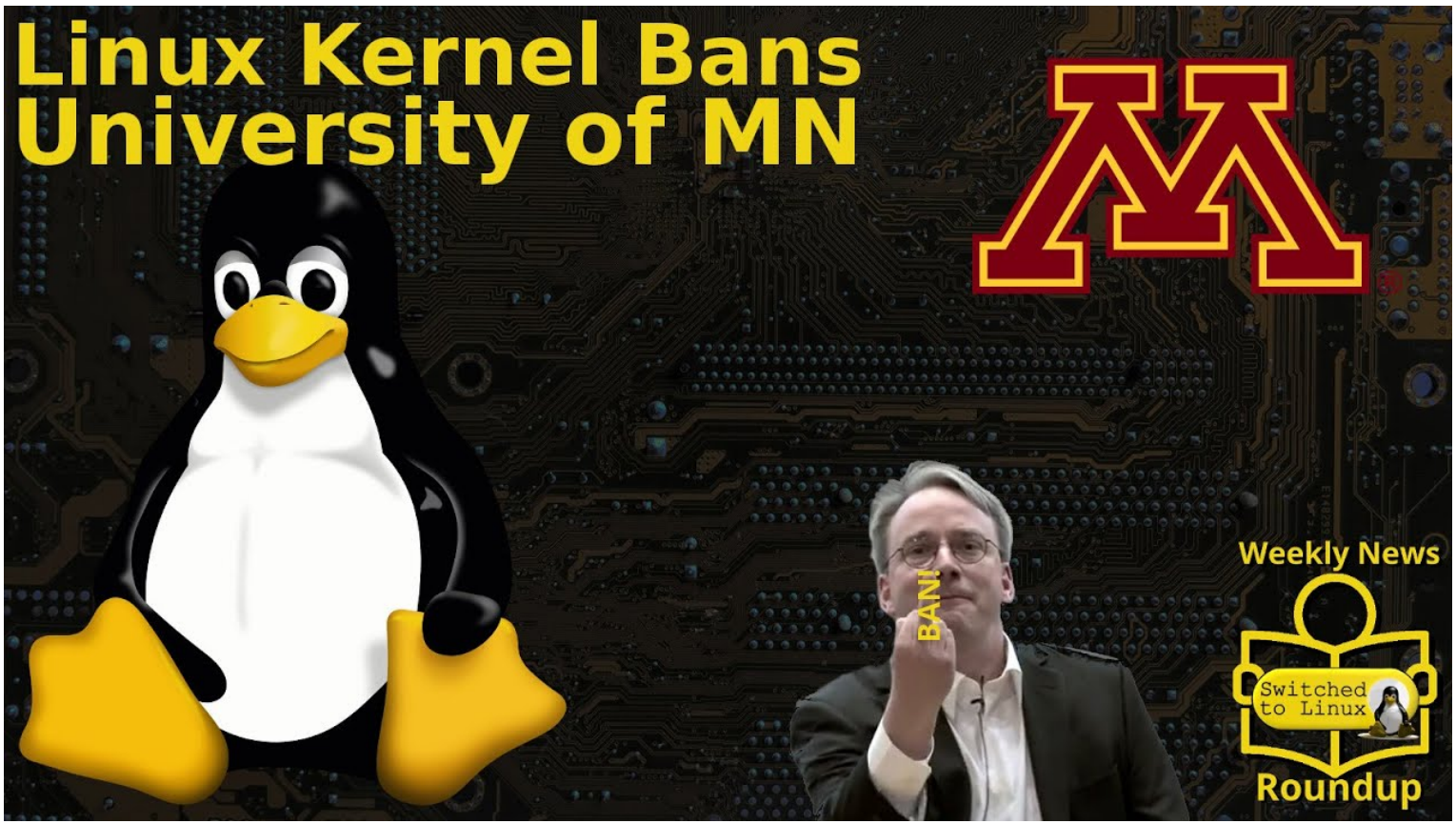
- You are an open-source enthusiast and make contributions to open-source projects regularly
- You are deeply concerned that the Linux kernel might be vulnerable to supply chain attacks due to its loose review process
- You want to remind the code reviewers that they should tight-up their code review practices
- So you send an intentionally buggy piece of code to the Linux kernel reviewer and ask for it to be merged into the upstream

Linux kernel and the University of Minnesota

- You are an open-source enthusiast and make contributions to open-source projects regularly
- You are deeply concerned that the Linux kernel might be vulnerable to supply chain attacks due to its loose review process
- You want to remind the code reviewers that they should tight-up their code review practices
- So you send an intentionally buggy piece of code to the Linux kernel reviewer and ask for it to be merged into the upstream

Q: How bad can this be?

Linux kernel and the University of Minnesota



What we learned from the examples?

Be extremely cautious when human is involved in any form of activity, regardless of physical or virtual presence:

What we learned from the examples?

Be extremely cautious when human is involved in any form of activity, regardless of physical or virtual presence:

- In three words: Think before action

What we learned from the examples?

Be extremely cautious when human is involved in any form of activity, regardless of physical or virtual presence:

- In three words: Think before action
- In two words: Think twice

What we learned from the examples?

Be extremely cautious when human is involved in any form of activity, regardless of physical or virtual presence:

- In three words: Think before action
- In two words: Think twice
- In one word: Don't!

What we learned from the examples?

Be extremely cautious when human is involved in any form of activity, regardless of physical or virtual presence:

- In three words: Think before action
- In two words: Think twice
- In one word: Don't!

Fortunately, we have laws and ethics to guide us on making a right-or-wrong judgement call.

Outline

Laws, morality, and ethics

Q: What are the commonalities between laws, morality, and ethics?

Laws, morality, and ethics

Q: What are the commonalities between laws, morality, and ethics?

A: They are all beliefs, claims, rules, and norms about how we should live and behave.

Laws, morality, and ethics

Q: What are the commonalities between laws, morality, and ethics?

A: They are all beliefs, claims, rules, and norms about how we should live and behave.

Q: What are the differences between laws, morality, and ethics?

What is law?

What is law?

- Laws are a set of formal rules that governs how we behave as members of a society.

What is law?

- Laws are a set of formal rules that governs how we behave as members of a society.
- The goal is to create a set of basic and objectively enforceable standard of behaviors.
- Specifies, in greater details, what we MUST do and more frequently, what we MUST NOT do.

What is law?

- Laws are a set of formal rules that governs how we behave as members of a society.
- The goal is to create a set of basic and objectively enforceable standard of behaviors.
- Specifies, in greater details, what we MUST do and more frequently, what we MUST NOT do.
- Laws are upheld and applied by a state-backed justice system.

What is law?

- Laws are a set of formal rules that governs how we behave as members of a society.
- The goal is to create a set of basic and objectively enforceable standard of behaviors.
- Specifies, in greater details, what we MUST do and more frequently, what we MUST NOT do.
- Laws are upheld and applied by a state-backed justice system.

Q: Why laws are not enough in the context of information security and privacy?

What is law?

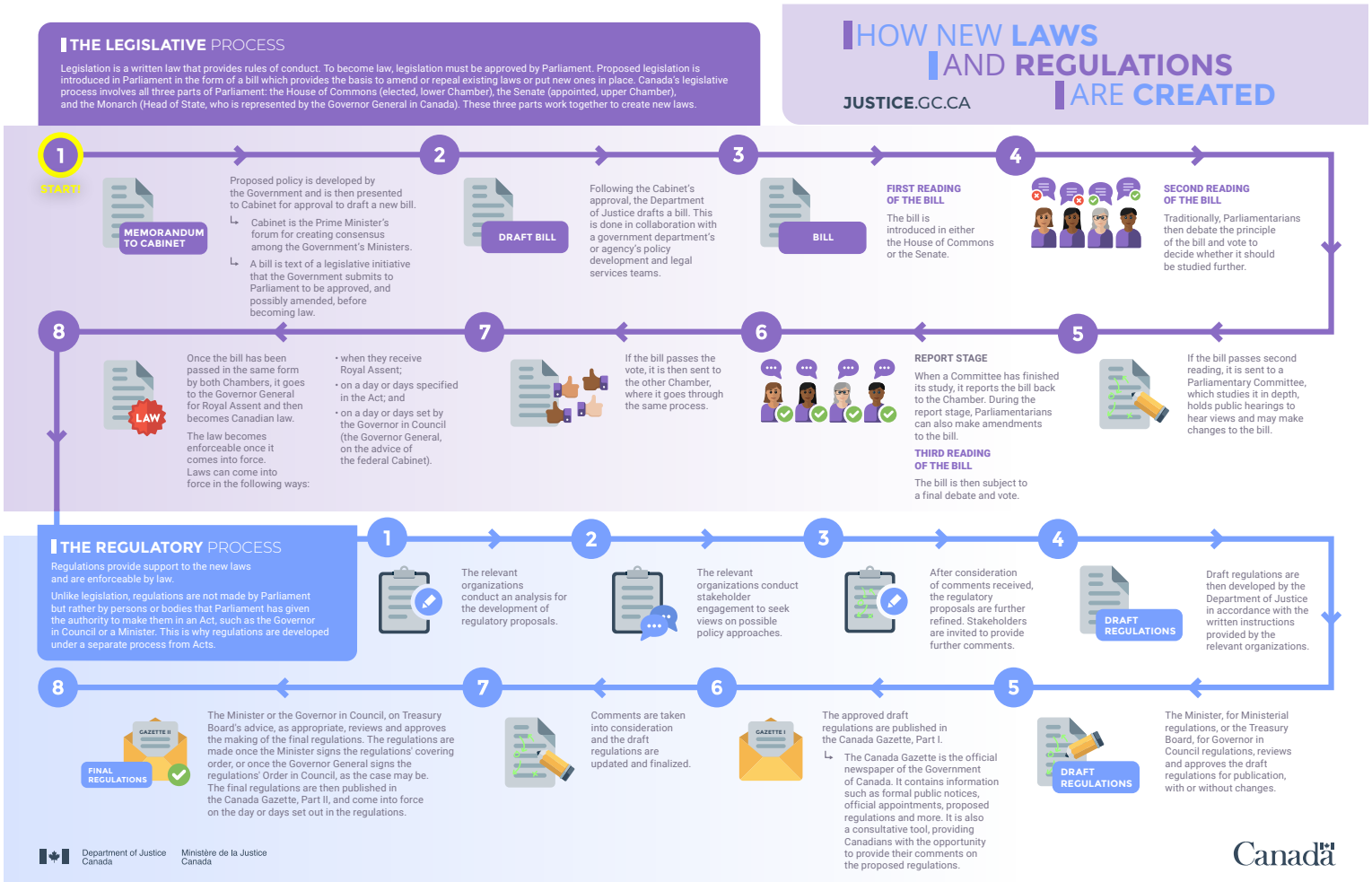
- Laws are a set of formal rules that governs how we behave as members of a society.
- The goal is to create a set of basic and objectively enforceable standard of behaviors.
- Specifies, in greater details, what we MUST do and more frequently, what we MUST NOT do.
- Laws are upheld and applied by a state-backed justice system.

Q: Why laws are not enough in the context of information security and privacy?

A:

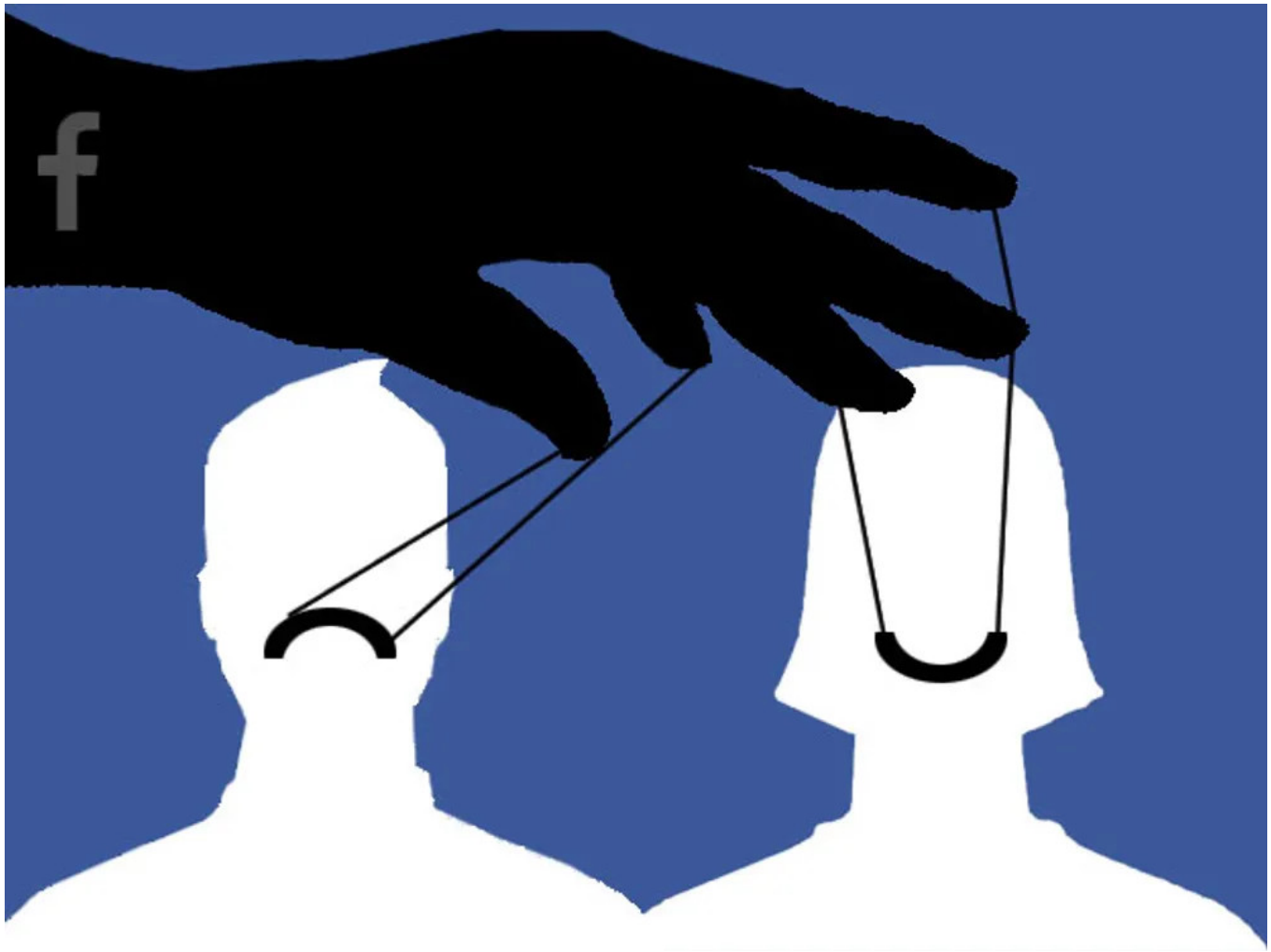
- The lengthy legislative process does not match with the fast-pacing tech industry
- Laws usually have a very narrow focus.

Lengthy legislative process



The legislative process in Canada

Non-violations of law



The (secret) mood manipulation study by Facebook in 2012

Some facts about the mood manipulation study

For one week in January 2012, data scientists in Facebook skewed the content of News Feed for 689,003 users.

- Some people were shown content with more positive words
- Others were shown content analyzed as sadder than average.

Some facts about the mood manipulation study

For one week in January 2012, data scientists in Facebook skewed the content of News Feed for 689,003 users.

- Some people were shown content with more positive words
- Others were shown content analyzed as sadder than average.

Finding 1: More negative News Feeds led to more negative status messages, as more positive News Feeds led to positive statuses.

Finding 2: Omitting (either positive or negative) emotional content reduced the amount of words the person subsequently produced.

Right and wrong

Q: Why there are no legal violations here?

Right and wrong

Q: Why there are no legal violations here?

A: Quoted from Facebook Terms of Service:

Product research and development: We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.

Right and wrong

Q: Why there are no legal violations here?

A: Quoted from Facebook Terms of Service:

> *Product research and development: We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.*

However, we might still have some upset feelings here.

What is morality?

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.
- An individual who is strongly bounded to a moral system may even consider questioning the moral system as wrong.

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.
- An individual who is strongly bounded to a moral system may even consider questioning the moral system as wrong.
- Usually, the process of moral formation is unconscious, e.g., by family, by community, or by culture.

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.
- An individual who is strongly bounded to a moral system may even consider questioning the moral system as wrong.
- Usually, the process of moral formation is unconscious, e.g., by family, by community, or by culture.
- The application of morality is almost a habit without an explicit thinking and reasoning process.

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.
- An individual who is strongly bounded to a moral system may even consider questioning the moral system as wrong.
- Usually, the process of moral formation is unconscious, e.g., by family, by community, or by culture.
- The application of morality is almost a habit without an explicit thinking and reasoning process.

Q: A legal + moral system to classify the rights and wrongs?

What is morality?

- Morality refers to an informal framework of values, principles, beliefs, customs, ways of living.
- Morality is usually not enforced by the state, but by social pressure to conform to moral norms.
- An individual who is strongly bounded to a moral system may even consider questioning the moral system as wrong.
- Usually, the process of moral formation is unconscious, e.g., by family, by community, or by culture.
- The application of morality is almost a habit without an explicit thinking and reasoning process.

Q: A legal + moral system to classify the rights and wrongs?

A: There is rarely a moral authority agreed by every individual

What is ethics?

What is ethics?

- Ethics is a branch of philosophy that answers a basic question: what should I do? (out of all possibilities)

What is ethics?

- Ethics is a branch of philosophy that answers a basic question: what should I do? (out of all possibilities)
- Usually, the process of making an ethical decision is a conscious reasoning process based on each individual's values, principles, and purpose — do something that is good, right, and meaningful.

What is ethics?

- Ethics is a branch of philosophy that answers a basic question: what should I do? (out of all possibilities)
- Usually, the process of making an ethical decision is a conscious reasoning process based on each individual's values, principles, and purpose — do something that is good, right, and meaningful.

What is ethics?

- Ethics is a branch of philosophy that answers a basic question: what should I do? (out of all possibilities)
- Usually, the process of making an ethical decision is a conscious reasoning process based on each individual's values, principles, and purpose — do something that is good, right, and meaningful.

- Ethics is the framework to reason about issues that the laws cannot or do not address
- Ethics is the framework to examine a moral system to see whether the principles and rules there make sense

What is ethics?

- Ethics is a branch of philosophy that answers a basic question: what should I do? (out of all possibilities)
- Usually, the process of making an ethical decision is a conscious reasoning process based on each individual's values, principles, and purpose — do something that is good, right, and meaningful.

- Ethics is the framework to reason about issues that the laws cannot or do not address
- Ethics is the framework to examine a moral system to see whether the principles and rules there make sense

In an ideal world, our ethical reflections shape the laws and moral systems a society will develop.

Outline

Responsible disclosure

Q: You have found a security vulnerability, what should you do?

Responsible disclosure

Q: You have found a security vulnerability, what should you do?

Coordinated vulnerability disclosure

Responsible disclosure

Q: You have found a security vulnerability, what should you do?

Coordinated vulnerability disclosure

- A private full disclosure to all responsible parties (e.g., software vendors for most software bugs)

Responsible disclosure

Q: You have found a security vulnerability, what should you do?

Coordinated vulnerability disclosure

- A private full disclosure to all responsible parties (e.g., software vendors for most software bugs)
- Wait for either a patch from the responsible parties of a specific amount of time (e.g., 90-days or 120-days)

Responsible disclosure

Q: You have found a security vulnerability, what should you do?

Coordinated vulnerability disclosure

- A private full disclosure to all responsible parties (e.g., software vendors for most software bugs)
- Wait for either a patch from the responsible parties of a specific amount of time (e.g., 90-days or 120-days)
- A public partial disclosure if you want to further pressure the responsible parties; or a public full disclosure in the interests of potential victims.

Build ethically

Build ethically

Tips for incorporate ethical decisions when building something new

- Get as many dissenting voices as possible.
- Explain how something works, what is possible to go wrong, and how bad actors can take advantage to a non-expert.
- The privacy and data protection norms and cultural values vary by region and country
- Consult other experts (e.g. ethics, religions, advocates, activists)

Talk to non-experts

Talk to non-experts

Talk to non-experts

If the tool works as intended?

- Who does this effect?
- Does this data need to be collected?

If the tool does not work as intended?

- Failure modes? abuse cases?
- Who does this effect?

Talk to independent experts

Institutional review board (IRB), a.k.a., independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), etc...

Talk to independent experts

Institutional review board (IRB), a.k.a., independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), etc...

is a committee that applies research ethics by reviewing the methods proposed for research to ensure that they are ethical.

Codes of professional ethics

You will probably be a member of one or more professional societies

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)
- Canadian Information Processing Society (CIPS)

Codes of professional ethics

You will probably be a member of one or more professional societies

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)
- Canadian Information Processing Society (CIPS)

These organizations have codes of professional ethics

Example: CIPS

These are the high-level bullets from CIPS' code:

- Protect Public Interest and Maintain Integrity
- Demonstrate Competence and Quality of Service
- Maintain Confidential Information and Privacy
- Avoid Conflicts of Interest
- Uphold Responsibility to the IT Profession

Outline

Legal protections

How can we defend against a threat?

- Prevent it: block the attack
- Deter it: make the attack harder or more expensive
- Deflect it: make yourself less attractive to attacker
- Detect it: notice that attack is occurring (or has occurred)
- Recover from it: mitigate the effects of the attack

Legal protections

How can we defend against a threat?

- Prevent it: block the attack
- Deter it: make the attack harder or more expensive
- Deflect it: make yourself less attractive to attacker
- Detect it: notice that attack is occurring (or has occurred)
- Recover from it: mitigate the effects of the attack

In addition to (sometimes instead of, unfortunately) using technological defences, we can also use legal defences

Overview of intellectual property

In contrast to real property, so-called "intellectual property" (IP) differs in important ways:

- It is non-depletable
- It is replicable
- It has minimal marginal cost

So the laws for IP differ from the laws for real property, and indeed are much more complicated

Types of intellectual property

Four kinds of IP here:

- Trade secrets,
- Trademarks,
- Patents, and
- Copyrights

Types of intellectual property

Four kinds of IP here:

- Trade secrets,
- Trademarks,
- Patents, and
- Copyrights

These four kinds of IP:

- Cover different intangibles
- Convey different rights
- Have different durations
- Use different registration process

Trade secrets

- This is the simplest kind of IP
- You want to protect some secret information
  - The formula for Coca-Cola
  - The method for computing how many airline seats to oversell
  - Your new O(n) sorting algorithm
- Just don't tell anyone, and call it a trade secret
  - Unfortunately, you have to tell someone, or it's not useful
  - You get legal protection if that person passes it on

Reverse engineering

- Reverse engineering is the process of taking a finished product and taking it apart to figure out how it works
  - If someone successfully does this and published the results, you've effectively lost your trade secret protection
  - General rule for trade secrets: it has to be a secret
- A similar rule applies to software, with some caveats we'll see later
- RC4 was originally a trade secret (a violation of Kerckhoffs's principle), but it was reverse engineered in 1994

Trademarks

- Trademarks protect names, brands, logos, and also domain names
- To get one, make a legal filing showing that you are using the name in commerce
  - This lets you sue others who use that name in a confusing manner
- Trademarks last while they are used (they have to be renewed)

Trademarks

- Trademarks protect names, brands, logos, and also domain names
- To get one, make a legal filing showing that you are using the name in commerce
  - This lets you sue others who use that name in a confusing manner
- Trademarks last while they are used (they have to be renewed)

Example: Microsoft vs MikeRoweSoft
Mike Rowe used to own the domain name "MikeRoweSoft.com"

Patents

- Applies to inventions (including algorithms), which must be:
  - Novel
  - Useful
  - Non-obvious
- The bargain is that:
  - You tell everyone how your invention works
  - In exchange, you get to have a monopoly over it for 20 years
- The most difficult form of IP to obtain

Cryptography patents

Many cryptographic algorithms are (or were) patented

- Diffie-Hellman (expired 1997)
- RSA (expired 2000)
- IDEA (block cipher used in early PGP, expired 2012)
- Lots of patents on elliptic curve cryptography

Since 2000, you could pick a good unpatented candidate of each type of crypto

NOTE: unlike trade secrets, this is not against Kerckhoffs's principle.

Copyright

- Copyright is the most well-known kind of IP
- Protects expressions of ideas in a tangible medium
  - But not ideas themselves!
- No filing requirement
  - But you can get additional benefits if you do file
- Lasts a "limited time"
  - Currently: life+70 years in the US, life+50 in Canada
- The copyright holder has monopoly rights over certain uses of the work; primarily, making copies

Outline

Cyber crime

- We saw that laws regarding intellectual property differ from those about real property
- Similarly, laws about unauthorized access o computers, networks, or services differ from those about physical trespass
  - But until those new laws came about, courts had to make really stretched analogies to handle such events

Cyber crime

- Early on, there were bizarre rulings:
  - The value of stolen data was the value of the paper it was printed on
  - The value of a stolen manual was the value of the equipment it was intended for
- Things seem to have settled down somewhat
  - GDPR:
    General Data Protection Regulation
  - PIPEDA:
    The Personal Information Protection and Electronic Documents Act
  - HIPAA:
    Health Insurance Portability and Accountability Act
- But there are still many recent and active issues!
  - If your ISP keeps a copy of your incoming email, is that wiretapping?

Rules of evidence

Another problem with prosecuting computer crime is producing evidence admissible in court:

Rules of evidence

Another problem with prosecuting computer crime is producing evidence admissible in court:

- Should the log files of the machine that was broken into be admissible?
- How should you preserve electronic evidence from the time of the intrusion to the time of a possible trial?

Rules of evidence

Another problem with prosecuting computer crime is producing evidence admissible in court:

- Should the log files of the machine that was broken into be admissible?
- How should you preserve electronic evidence from the time of the intrusion to the time of a possible trial?

Computer forensics replace regular forensics

Cybercrime treaty

- Worse, computer crime is often international (two or more jurisdictions)
- Rules of evidence, police powers, etc. in one country don't usually carry over to another
- The Council of Europe cybercrime treaty (to which Canada and the US are also signatories) stipulates that member countries should pass laws making it easier for law enforcement to access telecommunications traffic (including voice, data, and Internet)

Bill C-13 ("Cyberbullying Law")

Full name: Protecting Canadians from Online Crime Act:

- Really a "lawful access" law
- Passed in December 2014
- Any "public officer" (not just the police) can demand that any computer data in a person's control not be deleted (until a production order can be obtained)
- Lowers standard for seizing of computer data, transmission data, and tracking data to "reasonable grounds for suspicion"
- Provides immunity to ISPs that "voluntarily" hand over customer data to government
  - Even though the Supreme Court had recently ruled that unconstitutional!

⟨ End ⟩